תקן WS – GOV.IL

ל-GATEWAY הממשלתי

נספח ג' – תעודות דיגיטאליות -

CERTIFICATES

גרסה 2.3

מעקב גרסאות

מס"ד	תאריך	עודכן על ידי	תיאור השינויים
2.1	11.10.2015	אופיר יהב	זו גירסה 2.0 מספטמבר 2015 - בתבנית חדשה של ממשל זמין.
2.2	12.10.2015	אופיר יהב	הוספת הערה לחלק הכללי.
2.3	29.11.2015	יוני ארוך	שינוי לוגו והוספת נתוני גרסת המסמך

נתוני גרסת המסמך

גורם	תפקיד	שם מלא	תאריך	חתימה
נערכה ע"י	PMO	אופיר יהב	11.10.2015	(חתימה)
נבדקה ע"י	מוביל טכנולוגיות במערך סייבר ואבט"מ	אלעד פז	11.10.2015	(חתימה)
אושרה ע"י	מנהל מערך סייבר ואבט"מ	אברהם זרוק	11.10.2015	(חתימה)

תוכן עניינים

1. כללי

תקן ws.gov.il מבוסס על התקן העולמי ws-security המפרט כיצד ניתן לאבטח web services ע"י הזדהות ואימות המסרים העוברים בין השרת ללקוח.

תקן ws-security מאפשר מספר מנגנוני הזדהות, אך תקן ws.gov.il מאפשר הזדהות ע"י חתימה דיגיטלית בעזרת X.509 v3 certificate בלבד.

במהותו תקן ws.gov.il מחייב כל צד (שרת ולקוח) לחתום דיגיטלית כל מסר יוצא, ולוודא (verify) כל מסר נכנס. בנוסף, לכל צד יש רשימה של ישויות המורשים לפנות אליו, כך שבתהליך הווידוי, בנוסף לווידוא החתימה נבדק כי הפונה רשאי לפנות לצד זה.

מסמך זה מתייחס למערכות הפעלה שנמצאות במחזור החיים של Microsoft.

מסמך זה מפרט את הפעולות השונות לביצוע התהליכים הבאים:

1. התקנת תעודות ה-CA.
2. התקנת תעודת מכונה – Machine Certificate.

ממשל זמין שם לעצמו למטרה לאפשר ללקוחותיו, וכלל המשתמשים, שירותים מאובטחים ורציפים. מסמך זה כולל, בין היתר, הנחיות אבטחת מידע ודרישות טכניות הנגזרות מהן. רק הקפדה על הנחיות ודרישות אלו תיצור מעטפת הגנה מיטבית על השירותים ותשמור על רציפותם של השירותים.

2. מסמכים ישימים

תקן WS-gov.il. מסמך זה הינו חלק מתקן WS-gov.il.

3.התהליך

יש לעבוד לפי השלבים ולשנות (במידת הצורך) את ההגדרות לפי המסכים שיוצגו.

4. סרטיפיקטים

על מחשב שמשמש כשרת החושף Web-Services דרך רשת ה-gateway הממשלתית יש להתקין machine-certificate בעל יכולת להצפין ולחתום על מידע, שנחתם על ידי CA של ממשל זמין - תמוז.

נהלי ממשל זמין לא מאפשרים לבצע export ל-private keys של הסרטיפיקטים המונפקים על ידי ממשל זמין ולכן יש לבצע מתוך השרת עצמו בקשה להנפקת סרטיפיקט, לשלוח את הבקשה לצוות PKI בממשל זמין ולהתקין את התעודה שתתקבל. בנוסף על מנת שהסרטיפיקט יזוהה כמאושר יש להתקין את ה-public certificates של ה-CA של ממשל זמין. התעודות מותקנות כאשר מריצים את הסקריפט לבקשה ליצירת תעודה.

4.1 סדר פעולות להפקת Machine Certificate

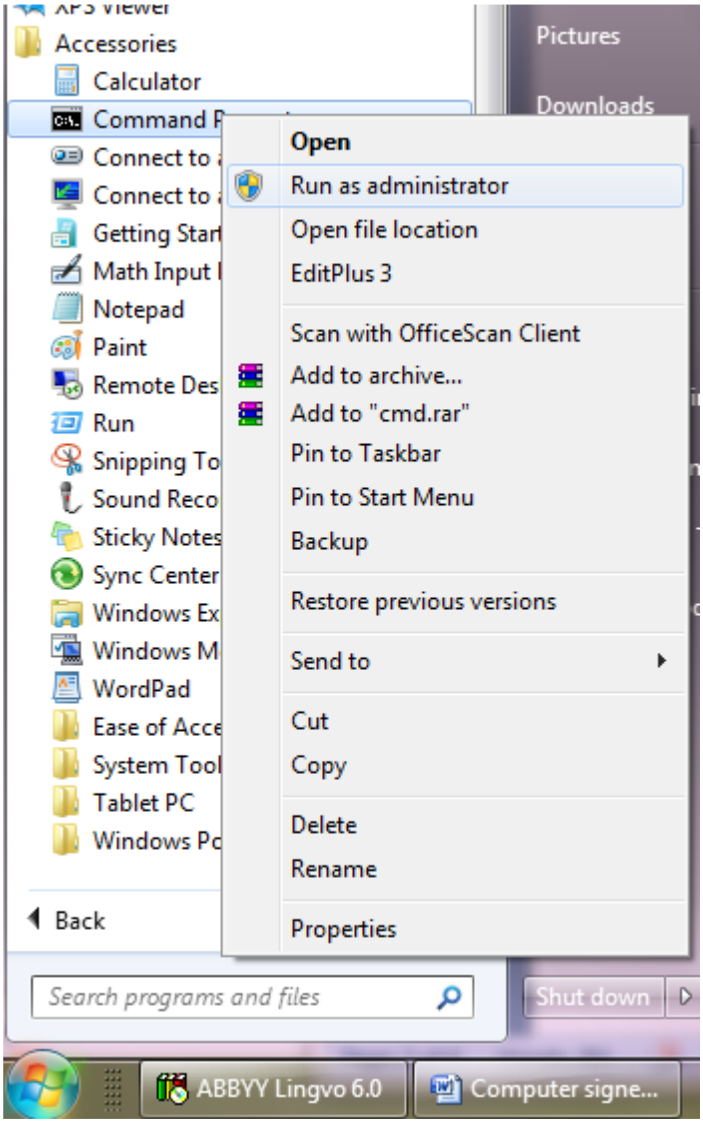
1. כאמור לעיל, אין תמיכה במערכות הפעלה שאינן נתמכות במיקרוסופט.
   ניתן לעיין בקישור המצורף https://support.microsoft.com/he-il/lifecycle

2. יש לגלוש לכתובת http://147.237.72.65/public/util/G2/Request ולהוריד את הקובץ הרלוונטי עבור מערכת ההפעלה: G2_Computer_Config_2008.zip עבור win 2008 ומעלה.

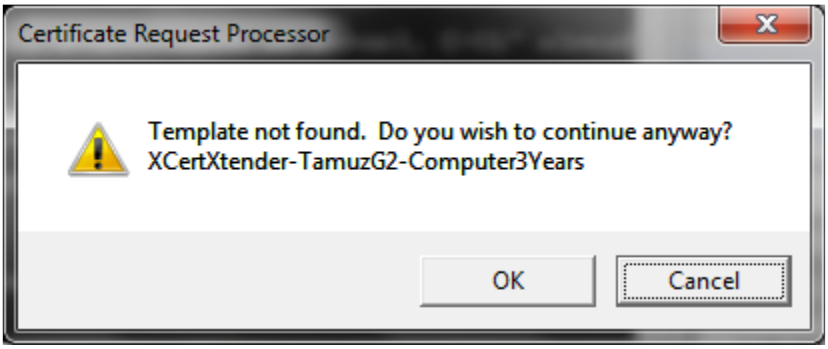
3. יש לשים את הקובץ על השרת/מחשב שעבורו רוצים לייצר תעודה.

4. יש לעשות Unzip לקובץ.

5. יש לעבור ל- Start/AllPrograms/Accessories/CommandPrompt וללחוץ על הכפור הימני ולבחור באפשרות של Run as administrator.

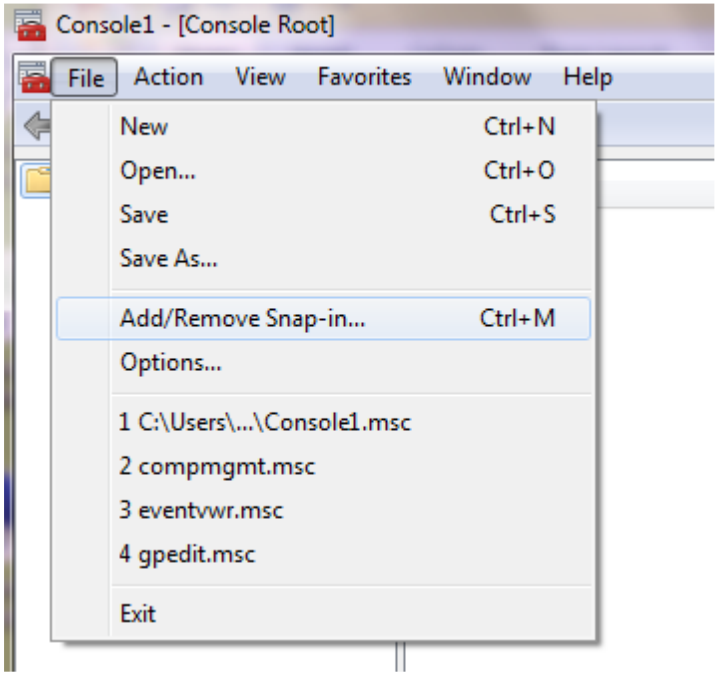


6. בשורת הפקודה עברו לתיקייה G2_Computer_Config_2008.
7. יש להריץ את הקובץ cert_request.bat.
8. לחצו על OK אם קופץ חלון.

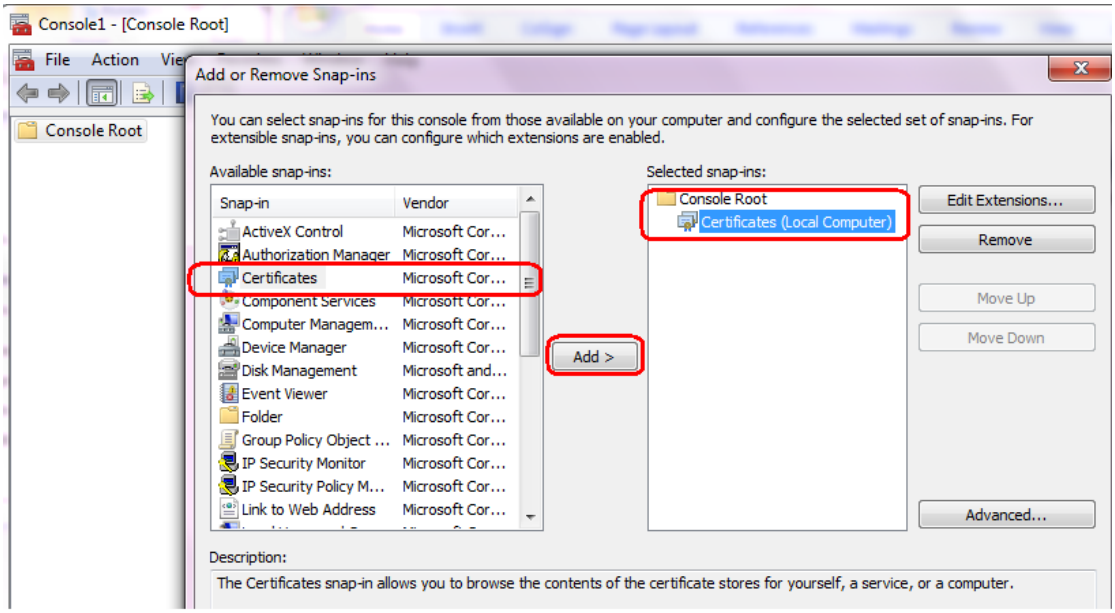


9. את הקובץ שנוצר בשם ComputerName.txt יש לשלוח לצוות SOA לחתימה. לנוחיותכם, רצ"ב כתובת האימייל SOAteam@gov.il
10. את הקובץ שנשלח אליך בחזרה מצוות SOA בשם ComputerName.cer.txt יש לשנות ל- ComputerName.cer.
   a) יש לשים את הקובץ ComputerName.cer בתיקיה Config_WS_2008
   b) יש להריץ את הקובץ cert_accept.bat (יש להריץ כ-administrator כמו בסעיף 4)
   c) יש לבחור באופציה OK כאשר יעלה חלון עם ההודעה הבאה:

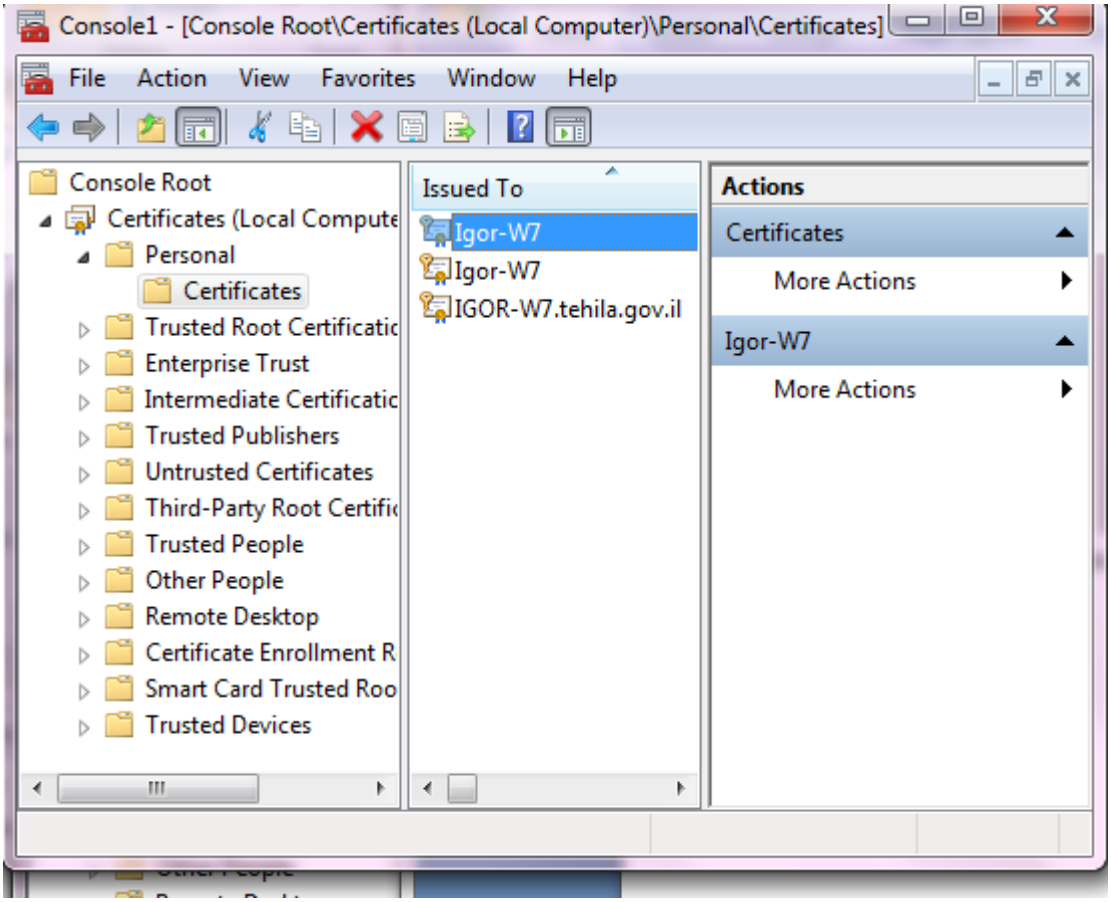
11. יש להריץ את – MMC (Microsoft management console) ניתן לעשות זאת באמצעות ה Run.
12. יש לבחור בתפריט של החלון שנפתח את File -> Add/Remove Snap-In…



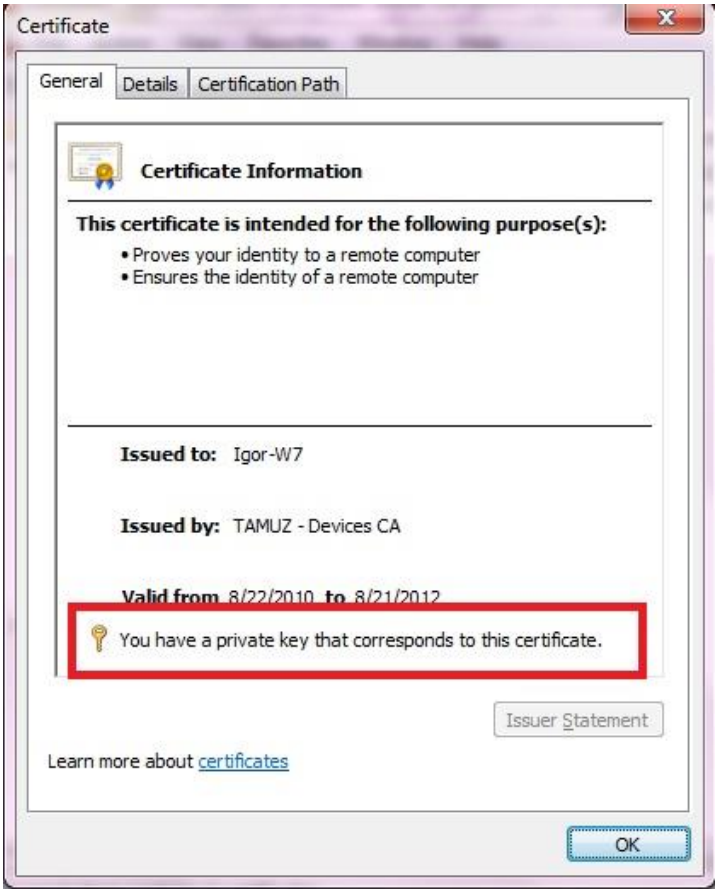
13. יש לבחור ב Certificates->ComputerAccount->LocalComputer



14. יש לעבור ל Certificates->Personal->Certificates ולבחור ב certificate הרלוונטי.

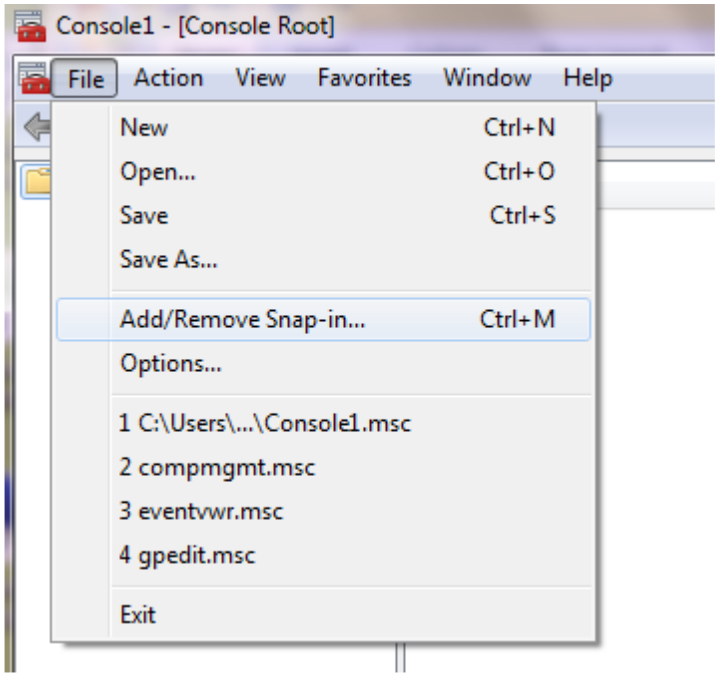


15. יש לפתוח את ה certificate ולוודא שיש private key.

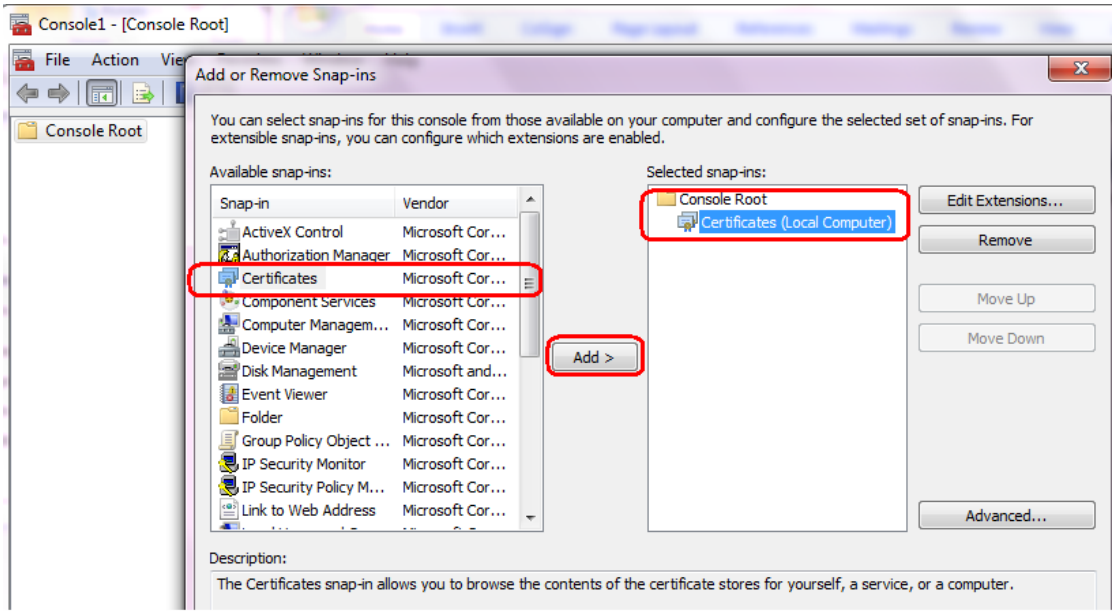


5. בדיקת הרשאות על תעודה

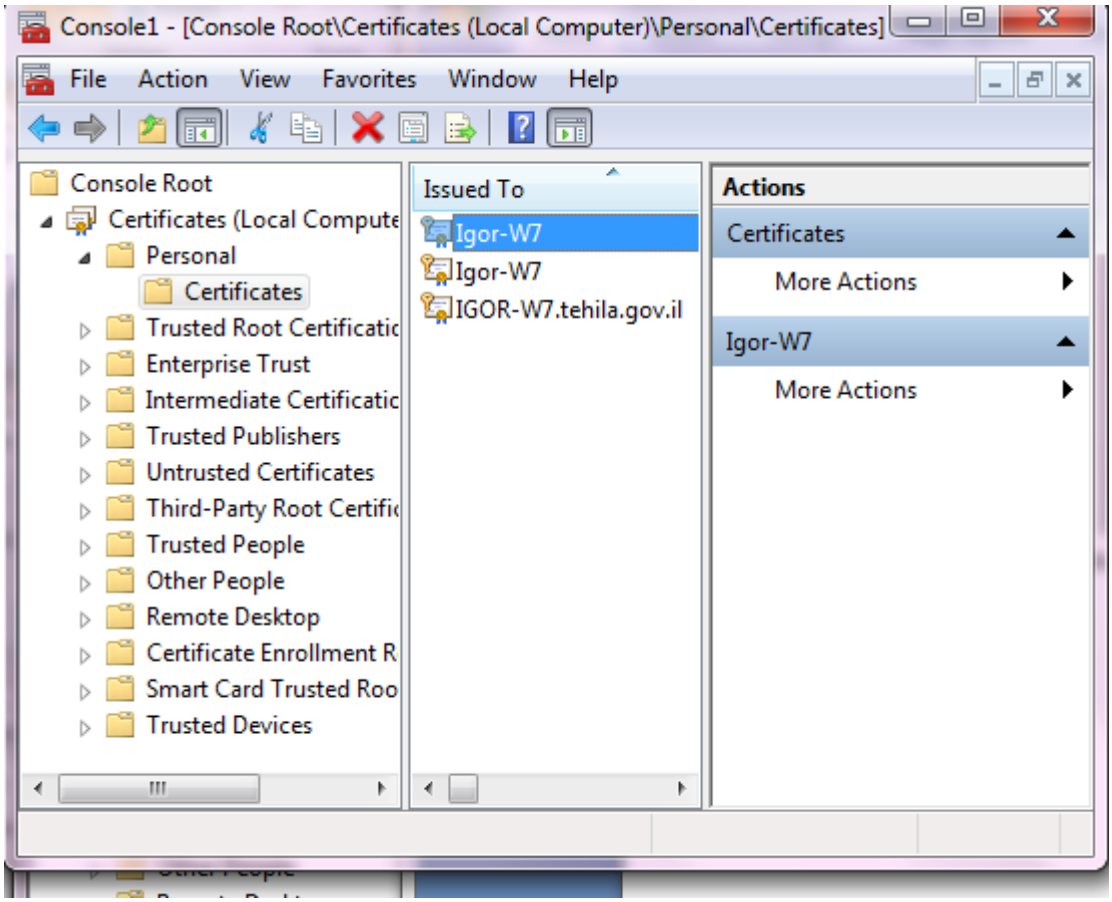
1. עבור מערכת הפעלה 2008 ומעלה:
   a) יש להריץ את – MMC (Microsoft management console) ניתן לעשות זאת באמצעות ה Run.
   b) יש לבחור בתפריט של החלון שנפתח את File -> Add/Remove Snap-In…



c. יש לבחור ב Certificates->ComputerAccount->LocalComputer



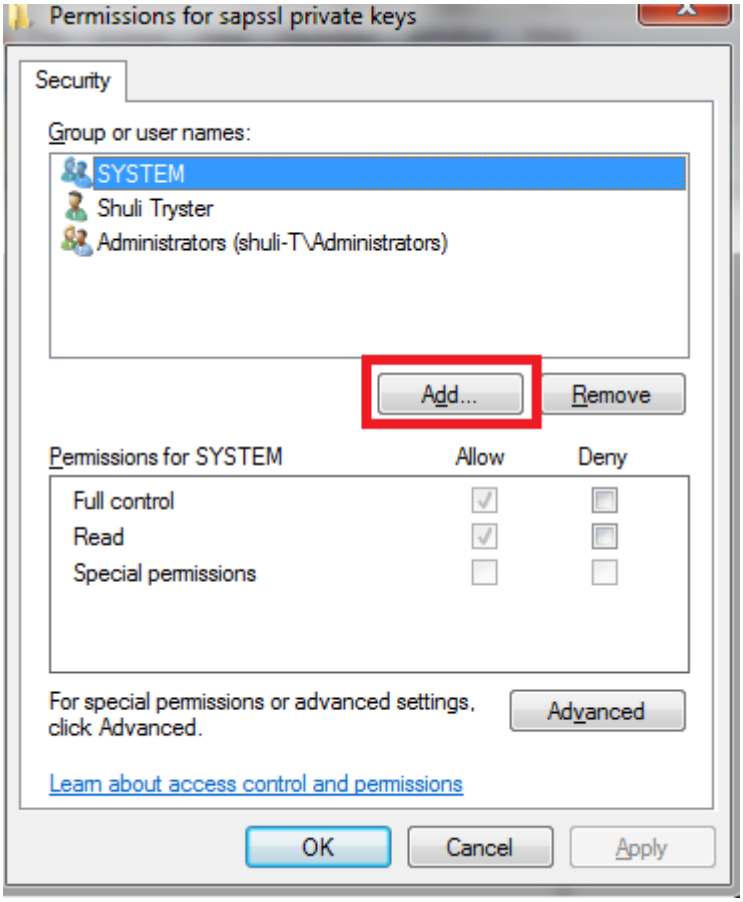
d. יש לעבור ל Certificates->Personal->Certificates ולבחור ב certificate הרלוונטי.



e. יש ללחוץ על הכפתור הימני בעכבר ולבחור ב-All Tasks ואז Manage Private Keys….

f. יש לבדוק האם למשתמש שמפעיל את השירות (ה- identity של ה-application pool) יש הרשאות Full Control על התעודה. אם אין, יש להוסיף את ההרשאות.

g. אם המשתמש לא קיים, יש להוסיף אותו ע"י לחיצה על כפתור ADD.



h. יש להוסיף את המשתמש ולתת לו הרשאות Full Control ואז ללחוץ על OK.